Defence Against Terrorism: The Evolution of Military Surveillance Systems into Effective Counter Terrorism Systems Suitable for Use in Combined Military Civil Environments. Dream or Reality?

C J Skinner, S Cochrane, M Field, R Johnston
AMS Ltd
Lyon Way, Frimley
Camberley, Surrey GU16 7EX
United Kingdom

chris.skinner@amsjv.com, stephen.cochrane@amsjv.com,
martin.field@amsjv.com, robert.johnston2@amsjv.com

ABSTRACT

This paper explores some of the issues surrounding the evolution of existing military capabilities, especially in the area of 'short-term' surveillance and threat assessment, where required reaction times may be counted in minutes or seconds and illustrate what can be achieved by reference to the development by AMS of a harbour protection system to address both civil and military requirements.

An understanding of the changing nature of the threat is key. The very lack of predictability means that it is much more difficult to bound the 'battlespace'. This in turn means that surveillance solutions will be required to cover larger areas over long timescales with a much more diverse set of 'targets', reliably and cost-effectively. The paper seeks to address to what extent existing military products satisfy these requirements through effective integration strategies and what capability gaps still need to be addressed.

The larger scale of the surveillance task is also likely to impose much greater demands on the human operators. This in turn can only increase the pressures to provide increased automation for fusion of data and information from a wider range of sources and automated situation assessment to provide timely warning of threats. These are key areas of research and development both within AMS and in the wider research community and ones where the development of counter terrorism systems could benefit significantly.

The development of harbour protection systems, based on a heritage of military surveillance, command and control systems serves to demonstrate the effective evolution of military technologies to meet defence against terrorism objectives. This approach shows how military technologies and the integration skills attained through their development are just as valuable in the civil domain and as dual use systems by civil and military organisations.

The key conclusions from this are that in this specific area it is not only possible but an effective approach to evolve civil and military equipments and capabilities to create systems that are effective in countering terrorism. It is also clear that those companies at the forefront of data and information fusion research will be able to contribute to an enhanced large-scale surveillance and threat assessment capability to counter terrorism without hugely increased demands on manpower and budgets.

1.0 INTRODUCTION

Whilst terrorism has existed through the centuries, it is often restricted to a region or country, usually involves demands and an escape route for the perpetrators, in many cases infrastructure is targeted and

Paper presented at the RTO SCI Symposium on "Systems, Concepts and Integration (SCI) Methods and Technologies for Defence Against Terrorism," held in London, United Kingdom, 25-27 October 2004, and published in RTO-MP-SCI-158.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
25 OCT 2004	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Defence Against Terrorism: The Evolution of Military Surveillance Systems into Effective Counter Terrorism Systems Suitable for Use in Combined Military Civil Environments. Dream or Reality?	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **AMS Ltd Lyon Way, Frimley Camberley, Surrey GU16 7EX United Kingdom**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM201977, Systems, Concepts and Integration Methods and Technologies for Defence against Terrorism (Systemes, concepts, methodes d'integration et technologies pour la luttre contre le terrorisme)., The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**22**	

warnings are issued to minimise casualties, as the killing of innocents usually alienates the public towards the terrorists. This has been transformed by the move away from small secretive terrorist groups to a global and relatively large-scale terrorist organisation attacking symbolic soft targets, infrastructure and the committing of mass murder by extremists that are prepared to die for their cause. A revised strategy is required to deal with the new brand of terrorism and emphasis on good intelligence and sufficient warning to act against terrorists before they strike. In this paper we explore some of these issues and the technological responses needed.

Military forces are established to defend their States and project force as necessary to protect overseas interests, not specifically to deal with terrorism. The role of protection against terrorism is often a civil issue. Defending Sovereign States against terrorism will require a co-ordinated civil and military response, integrating the capabilities and processes that exist in these separate domains with an effective command and control doctrine and integrated system of systems approach. Given the scale of investment in military surveillance systems designed to inform the commander on the status and threat posed by his adversary, it is clearly preferable that we should evolve existing capabilities to address these changing requirements. Starting again is not a realistic option. However, the nature of the threats are such that not only is the surveillance requirement 24/7 but the quantity of data is such that threat analysis and alerting operators to potential threats will be the only way to move towards a real time system that allows verification of a target and sufficient time to act upon the information thus preventing a terrorist event. Populations, civil agencies and assets (both physical and fiscal) will all play a critical role in countering terrorism and these resources must also be harnessed.

An understanding of the changing nature of the threat is key and will be discussed in Section 2. The very lack of predictability means that it is much more difficult to bound the 'battlespace'. This in turn means that surveillance solutions will be required to cover larger areas over long timescales with a much more diverse set of 'targets', reliably and cost-effectively. The paper seeks to address to what extent existing military products satisfy these requirements through effective integration strategies and what capability gaps still need to be addressed.

All countries and populations are facing the new terrorist threats directly or indirectly, as all nations depend on trade for economic prosperity. Economic prosperity in turn relies on stability and security; the negative impact on the global economy post 9/11 is well documented, as is the rise in oil prices related to the Iraqi crisis. The threat of instability and terrorism is costing the Global economy billions of dollars and therefore it is in all nations interests to act quickly against this new brand of terrorism. However, the resources, development of counter terrorist systems in the broadest sense and training all take time and require an apparently unaffordable expenditure. It is therefore essential to maximise the use of existing assets and prioritise the requirements and capabilities that will provide nations with the greatest ability to counter threats and achieve the effective resilience in the inevitable event of a successful terrorist event. Effective real-time intelligence, threat assessment and efficient Command & Control are essential.

In Section 3 some of the issues surrounding the evolution of existing military capabilities, especially in the area of 'short-term' surveillance and threat assessment, where the required reaction times may be counted in minutes or seconds, are explored. We illustrate what can be achieved by reference to the development by AMS of an anti-terrorist force protection system to address both civil and military requirements. The rapid prototyping of a Force Protection solution was based on threats to ports and harbours, the need for protecting ships at anchor and supporting infrastructure. This paper considers some of the specific requirements that need to be addressed in this context. The paper also takes into account the technology available and the need to use proven and reliable products and capabilities and considers the problems associated with defining the threats so that the systems can perform accurate threat assessment to alert the operator. Defining the threat of an asymmetric attack is complicated by the fact that such an attack is infinitely variable in its nature and location.

In Section 4 we address the issues relating to development of new system concepts and the role that simulation and synthetic environments can play here. The ability to investigate different concepts and architectures in synthetic environments will be key to developing a deeper understanding of the threat and the potential counter solutions. It is clear that system architectures will be an important issue and open extensible architectures are an important enabler in this respect.

Section 5 investigates some of the technology requirements and emerging solutions that will enable us to provide better solutions in the future. The emphasis here is on improved automation leading to reduced reliance on the human operator for routine surveillance and threat assessment.

The conclusions make it clear that technology has a major role to play in building new system concepts for defence against terrorism and that there is much that can be taken from mature military capabilities. The concept of evolving military solutions to meet terrorist threats has been demonstrated successfully in the example of a force protection system and this shows the way forward in addressing a wider range of problems.

Anyone or thing that threatens global security, stability and prosperity must be countered in the broadest sense as it affects us all directly or indirectly. This paper aims to broaden the discussion and uses a practical example to illustrate how an intelligent surveillance system can help identify a threat, alert an operator and provide valuable time for resources to be directed to counter the danger.

2.0 THE CHANGING NATURE OF THE THREAT

2.1 The new threat and its implications

The 9/11 attack on the world trade center is the most dramatic example of the new terrorism. But is it an isolated singular event or part of an evolving pattern? If we concluded that it was a singular event then there would be no need for a radically different plan of action beyond what has traditionally been done to counter terrorism. Unfortunately there is evidence that suggests an evolving pattern that points to growth of new asymmetric threats. These considerations are discussed below.

From the actions of Al Qaeda, three core characteristics can be abstracted and seen to apply more generically:

Audacity - Targets of maximum symbolic impact are chosen. Most hijacks in the past have involved getting the plane back on the ground and then negotiating for the release of the passengers and crew as hostages against a list of demand and usually an escape route. Typically hijackers fail, as their demands are not met. The authorities concerned know very well that giving in to these demands will be seen as a sign of weakness and is likely to make them a target for further incidents. The 9/11 attack is clearly very different in this respect. The simplicity of the 9/11 concept, once there was the commitment to achieving it, is part of its impact and the shock that it generated. The dramatic destruction of the towers may or may not have been envisaged but the target was chosen as a major symbol of the USA global trade empire. Not only was it symbolic but 3000 people were killed[1], making this the most effective terrorist attack by far. In this case and Madrid, Al Qaeda differ from most terrorist groups in that they are global, innovative in their choice of targets and co-ordinated means of attack and prepared to commit mass murder and die in the process.

Co-ordination and Planning – Prior to 9/11 the presence of Al Qaeda was scaled up over a number of years. Each individual preparatory action for 9/11 was, when taken alone, harmless and involved only

[1] The sarin nerve gas attack in Tokyo, 20th March 1995 caused 5511 casualties but only 12 killed. This shows the potential reach of chemical or biological attack.

minor deception but accumulated into a major effect. The means of destruction were effectively supplied by the victims in the planes themselves (chosen to be long-distance because that maximises the fuel load) and the nature of the buildings that are both a target and the extended means for amplifying the devastation. There was no leak and the structure of the plan gave rise to a co-ordinated attack but with each hijack group on individual planes acting autonomously.

Levels of self sacrifice – In contrast to the usual dispossessed or deprived terrorist recruit, educated and skilled people, living in the west were apparently assimilated, but harboured deeply held beliefs that were antagonistic towards the USA to the extent that they became willing martyrs for those beliefs. Security procedures where and are still vulnerable to the suicide attacker but this Al Qaeda plot did not have to exploit that weakness because the means of destruction were supplied by the victim country.

Although it is not to be expected that this precise template will be followed in successive attacks, with innovation being a hall-mark of Al Qaeda strikes, the characteristics of *audacity*, *co-ordination and planning*, and *self-sacrifice* can be applied. Therefore this new situation needs to be assessed and an effective plan of action devised. The nature of the problem means that it is difficult in a democratic society to devise and implement a rational and well-founded plan without having a greater psychological impact than the objective risks warrant. The imagination sees no bound to the potential destruction but does this mean that we are in a war situation?

Terrorism is a tactic, not an opponent. Declaring a "War on Terrorism" is at best a rhetorical stance and dangerously a legitimisation or even glorification of terrorists. The UK, as well justified policy, did not seek war with the IRA nor Spain with ETA, though both are well-organised terrorist groups. They are groups that could be contained by their local aspirations. The current threat has global reach because the terrorists are tied to a world religion and more importantly because of the global presence of western interests and values. It is an outcome of globalisation that it has so eroded the effects of distance that any terrorist group can reach targets over intercontinental distances. Proximity is not always a danger. If ETA is not a threat to the UK, it is not because they cannot get here nor because they could not build a network here if they so chose. Reach is not the constraint but intent is: our enemies are those whose intentions include killing us, striking at our social structure or our essential infrastructures. This has remained a constant in security assessment and a realistic evaluation of what these groups are and what their capability is remains key. However the inability to bound the threat geographically is a further characteristic of the new situation given the global mission of the terrorist network with recruiting pools across the world.

Even if there is no formal war there is a new threat and terrorism is the tactic being used but what is the nature of the threat? Attacks such as 9/11, for all their devastating impact are not critical blows to civilisation. Kinetic attacks (truck bombs or crashing planes) do not scale up to the point of dealing a critical blow to civilisation but other methods could and may not be confinable. Other means of terrorist attack could have profound impact through disruption to trade and destabilisation of national economies.

The characteristics of audacity, planning and self-sacrifice can be applied to other more devastating means of attack. Nuclear or chemical (including dirty bombs) attack would mean the loss of life and property on the scale of a city or a region but a biological attack could take advantage of natural propagation mechanisms to achieve global devastation. More subtle but perhaps equally effective would be major attacks on infrastructure leading to the breakdown of supply and eventually social order at the national level. As outlined in Section 3 critical infrastructure nodes and other vulnerable high profile targets could be protected by extending methods that are available today.

An alternative scenario is that the Al Qaeda game plan is not to cause large-scale devastation in a western country by terror tactics but to achieve the psychological conditions for destabilisation of a nation and to gain control of that country. The levels of panic achieved so far do not give any reason to think that a

western nation will succumb to this destabilisation but it is conceivable in less stable parts of the world. Once in charge of a country they may continue to use global terror tactics but to scale up their activity they must move to more conventional state based means of attack. In addition they then provide the missing geographical focus for a military response. This then becomes a less ambiguous war scenario in which the west has overwhelming advantage. The danger, however, may not be in losing the war but in a key component in the global economy being eliminated.

The assessment of risk of a major impact terrorist strike is difficult because of the asymmetry of the situation.

- The terrorist community is a small sub-set of current pools based on religion or ethnicity.
- The terrorist is successful if one of many attempts succeeds.
- There are no bounds to the battlespace and attempting to define secure interfaces erodes liberty and merely moves the threat to another point of penetration
- Unpredictability is a major issue. Attack could be anywhere and anytime with deception as a key attribute

Some classification and evaluation scheme is required to assess impact and put in place mitigation plans.

2.2 Identification and Analysis of Candidate Threats

The threat should be understood as a combination of perpetrator, means, target and impact. Without one of the four there is no significance to the threat and by identifying candidates for each of the first three we can construct possible scenarios and estimate the impact. Some initial steps have been taken along these lines by Woodcock [[1]]. If this approach is to be developed to a full evaluation system then its output would be very sensitive information. As would the steps taken to mitigate the impact.

Scenarios may be generated by breaking the problem down into lists for:

Perpetrators – Individuals, small ethnic groups, small religious groups, local groups, global groups etc.

Means – Suicide bomb, car bomb, dirty bomb, nuclear bomb, missiles, biological infection, information attacks etc.

Targets – Symbolic (Buckingham palace), economic (City of London), infrastructure nodes (M25 critical intechanges), government buildings, military installations, religious centres, etc.

Even at a simple level this suggests frameworks for scenarios that may not have seemed obvious but it is clear that more input of imagination and analysis is required to provide aids to policy or acquisition of systems and equipment. Even ignoring the “etc.” in the short lists above, simple combination provides 375 potential scenario outlines that can be populated in countless ways e.g. there are other key roads, railways, shipping, water, electricity, gas, food, health and airports.

A combination of intelligence, debate, simulation and judgement can then brought to bear to prioritise the threats and develop response mechanisms. The identification of maximum impact is a shared goal of the terrorists and the attacked. The terrorist will seek to carry out the threat of maximum impact and the attacked to mitigate that impact by counter measures, eliminating the means of attack, or either protecting or derisking the candidate target.

With the 9/11 attack a terrorist group has shown it has not only the intent to inflict unprecedented damage (for a terrorist organisation) but has shown itself capable of the **Audacity –** to innovate and strike a target

of maximum impact, of the **Co-ordination and Planning** – to build up slowly, stealthily and securely, and demonstrate **Levels of self sacrifice** – recruiting educated and skilled people appearing to be assimilated in the west.

This means in practice that there is greater need for intelligence and situational awareness as part of the overall assessment and early warning capability. Our simple threat breakdown shows that this is a very wide-ranging problem. There is the need to track suspect individuals and groups, and materials and to protect high profile targets. The evaluation of risks to assets and insight into the networks of events that could accumulate in a large-scale breakdown in security resulting in massive human, material and psychological damage is needed.

It is not possible within the scope of this paper to address this breadth of threat and mode of attack. For some of the problems identified it is difficult today to identify a solution (both in organisation and technical respects) and there is an urgent need for research. In others cases feasible solutions that address at least some of the requirements can be conceived of today and this paper uses an example of such a solution to explore the exploitation of investment in military systems to provide solutions.

A matter of great concern is the potential for terrorist action to impact on the economy of NATO nations either through attack on financial institutions or through key trade routes. Maritime trade is a vital element in this respect with up to 90% of the world's trade travelling by sea, much of it through ports and territorial seas of NATO and allied nations. This threat has been highlighted in [5] which addresses terrorist threats against both civil and naval shipping targets in and around ports and harbours and specifically describes the need to "transform harbours into safe havens for ships".

The assessment in recent EU studies on security [4] also identifies a clear need for a technological response as an essential element in maintaining security and has recommended a significant programme of security related research. In AMS we have already recognised the immediate need for surveillance systems. In the short term there is, for example, the InSITE force protection system that AMS has developed for harbours and other installations (Section 4), which could be extended to key infrastructure nodes, power stations and some public buildings. Dealing with the wider threat set, discussed above, will require extending traditional threat assessment and decision support techniques and systems. To be effective this will also need the support of training, simulation and processes.

3.0 ANTI-TERRORISM FORCE PROTECTION

The advent of these new terrorist threats described above raises vital questions about the best type and style of response and protection. By their very nature these threats, and critically the organisations behind them, are almost impossible to counter at their source and at best any attempt to do so will be a long term strategy. Even if it were considered possible to destabilise and defeat Al Qaeda we could not be confident that another organisation using similar tactics would emerge in its place. In short we may be entering a period of history characterised by global threats from disaffected minorities. An intelligence led approach will be essential in helping to identify specific threats of terrorist action, and in allowing defensive efforts to be applied most effectively. Another element of the response will be the provision of protection for high value assets (military, governmental, transport, trade etc) in that these will always be likely targets for terrorist action and could offer the greatest impact. Both of these two approaches can benefit from a high level of technical maturity in equivalent defence capabilities – where very similar problems have been encountered.

The type of solution described in this section falls into the second of these two categories and is concerned with the protection of nominated assets from terrorist attack. In part it is based on identifying and intercepting attacks before they become effective and cause any damage. In part there is also a deterrent

element – if the potential attackers believe that the protections in place are effective they are more likely to seek a more accessible target elsewhere. As such it only represents a partial solution to the problem – in a sense simply pushing it elsewhere.

The development of harbour protection systems, based on a heritage of military surveillance, command and control systems serves to demonstrate the effective evolution of military technologies to meet defence against terrorism objectives. This approach shows how military technologies and the integration skills attained through their development are just as valuable in the civil domain and as dual use systems by civil and military organisations.

3.1 The military surveillance, command and control approach

Most of the established military solutions to the command and control problem have their origins in a cold war type scenario where the emphasis was very much on technological superiority. This same approach has been shown to be of great benefit in recent conflicts and is still one of the key principles adopted by our nations today, although perhaps with a slightly different emphasis.

In the past the emphasis has been on a more symmetrical conflict and from a technological approach this means being able to field capabilities similar to those of the opponent but better (faster, longer reach, more difficult to detect). Speed of attack and response have been key drivers and this in turn has created the demand for effective integration across the different components of a force.

The surveillance, command and control systems in use today reflect this. They are optimised to take inputs from a range of highly sophisticated sensors, provide the decision makers with an accurate and up to date picture of the battlespace and provide the facilities to engage enemy threats quickly. Naval platform combat management systems are an excellent example of such capabilities. These systems combine the inputs from a range of sensors (radars, sonar, EO and ESM) plus off-platform data sources to provide a tactical picture updated in real time combined with the ability to control the platform's weapon systems.

In these military systems the requirement drivers have been speed of response and quality of the tactical picture. Some of the key aspects being

- Inclusion of all the relevant threats
- Clarity to the operator – maximising his awareness of the evolving situation
- Accuracy of the picture to the real world it represents
- Stability and consistency of the picture

Survivability is an important element in achieving combat success and the military systems have been build with this as a constraint – and they offer high degrees of resilience and reliability even when operating in difficult and demanding conditions.

Military success depends very much on the ability to co-ordinate across the force – increasingly so as we become more reliant on coalition type operations. Interoperability and the ability to exchange information across the force are therefore key considerations and this is reflected in the degree of standardisation that has been achieved within NATO.

3.2 Harbour Protection – Understanding what is different from the military problem

It will become clear that there are many similarities with the military surveillance problems discussed above – but equally that there are differences and these impact on the requirements that need to be

addressed. These differences stem mostly from the nature of the threats, but also from the organisational issues relevant to protecting commercial harbours and ports.

The conventional military threat would be delivered by air (aircraft attack, missiles etc) or by sea (missiles, torpedoes etc) and would be launched from platforms that are relatively easy to detect and classify from some distance. The targets for attack would be military platforms whilst in harbour and the associated military infrastructure. A good prevention approach is to establish and enforce a large exclusion zone.

There are some key differences to be considered for the asymmetric or terrorist threat. The attack could be delivered by air, land or sea (surface and underwater) but will often not be identifiable as a threat until at relatively short ranges. Attack from the air could for example be from a hijacked aircraft, or from a innocent seeming light aircraft. From land the attack could use a disguised vehicle carrying explosives entering the port under false identification or a weapon such as RPG launched at modest stand-off range. Attack from the water could be a small ship carrying undeclared explosives, a small fast attack craft, low cost mines deployed in the harbour or divers delivering improvised explosive devices. Both conventional and unconventional (chemical, biological, nuclear) devices might be used. In all these cases the threat is most likely to emerge locally from a disguise that implies some legitimate activity.

Figure 1. The difficulty posed by the new threats is that many seemingly innocent vessels and activities may disguise the actions of terrorists. Physical attributes may not be sufficient to distinguish the threats from the legitimate. Poor weather conditions and night time operations will further hinder the identification process.

The targets for attack could be both shipping in a port or harbour and any element of the port infrastructure – in that the objective of the attack is as likely to disrupt the commercial activities of a port as much as to cause specific damage. There is also the added factor to consider in the role of ports and harbours as entry and exit point and the need to control the movement of people and materials. Denial of access for legitimate purposes through perceived threat could be almost as disruptive as destruction of the assets concerned but is easily achieved in an atmosphere of fear and uncertainty.

The users of these systems will not necessarily be the military – but may be from a mixture of civil agencies. Their skill levels, background, experience and skills are all likely to differ from established military. It is likely they will be operating in a different style of command structure and have different expectations and prejudices compared with the military.

There are some important practical implications of these differences:

1. The surveillance problem is generally much more difficult. The number of 'potential threats' is much larger (as discussed in Section 2) and there will in general be much more 'noise' to confuse and distract.
2. The detection and identification process is much more difficult because much greater use will be made of deception techniques. Classification based on physical characteristics will not be sufficient to determine what is a real threat. Earliest possible reliable identification is essential – the greater the warning time the more likely the threat will be successfully neutralised.
3. The number and type of sensors used is likely to be larger potentially generating more work for the operators. It may also be necessary to interface with existing surveillance systems – for example vessel traffic management systems.
4. Information sources other than conventional sensors are likely to play an increasingly important part in the classification and threat assessment process. These could include historical records, intelligence information, data from other ports, vessel history.
5. The potential to be overwhelmed by false alarms and indications is very large – and the consequence of incorrect identification and action are if anything less acceptable. It may be necessary to modify the policy on false alarms according to a declared 'alert state'.
6. The need is for continuous monitoring 24 hours a day for anything suspicious or unplanned. Extensive reliance on the human operator to achieve a high degree of vigilance and reliability is probably unrealistic.

All of this is likely to place greater demands on the operators compared with equivalent systems – in a context where the operator community is likely to be less well trained, less homogenous and perhaps under greater pressure than the military.

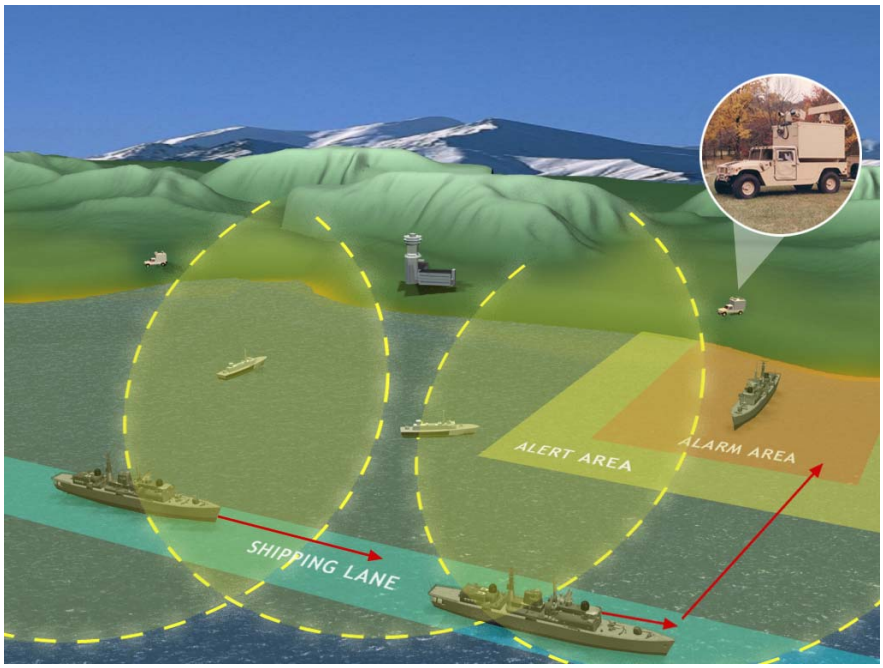

Figure 2. Effective surveillance of high value assets in ports and harbours requires inputs from a range of sensors and the ability to establish protected areas.

The implication is a much greater need for automation and decision support than has been the case to date. Specifically the need is for technology that will help in the following ways :

- To reduce the human burden of the surveillance problem and reduce the risk from poor concentration and attention.
- To assist in the fusion of information from multiple sources such that the operator is provided with the best assessment of the situation as quickly and reliably as possible.
- To reliably prioritise threats based on all the information available (reducing the number of false alarms) and to recommend the best course of action.

These are all areas where some capabilities exist today but where there is a significant investment being made in relevant research and we would expect much improved capabilities to become available over the next few years.

AMS has produced the command and control element of an anti-terrorist force protection system, working with DRS. This C2 capability (called InSITE) is based on the latest technologies taken from our Network Enabled Combat Systems for naval platforms and is initially targeted at protection of assets in ports and harbours. It is suitable for fixed installations, ships at anchor, near shore shipping traffic, and civil infrastructure protection – including temporary facilities and specific events.

The naval combat management systems provide many of the attributes required in such a system, in particular an architecture capable of supporting the required functionality and providing flexibility and many of the core application elements. This can be supplemented through the addition of more sensors, new applications and greater automation. The key here is the provision of a highly capable integrated system that has the potential to deliver a solution with acceptable manning requirements and to link with a wide variety of data sources including existing infrastructures such as a vessel traffic management system.

The force protection system uses a wide range of fixed and mobile sensors to monitor local traffic and automatically raise alerts when threats to nominated defended assets are detected. It is a genuinely

networked capability allowing multiple surveillance sites to be linked together and share information. This allows off-shore patrol vessels to contribute to the surveillance activities and provide part of the defence mechanism.

The range of sensors that can be supported includes :-

- Radar providing surface and air defence coverage. Mobile installations allow surface coverage to be optimised.
- Electro-optical devices including video cameras. A mixture of visible and infra-red coverage provides a degree of day/night coverage. Both fixed sensors (covering important locations) and remotely controlled sensors may be used. High resolution optical sensors have a relatively poor field of view and are best used in conjunction with other sensors to collect detailed information used to aid in the classification process.
- Sonar sensors for underwater surveillance.
- AIS systems to provide a positive identification from vessels equipped with this capability.

There will also be other inputs derived from radio traffic that may need to be manually input.

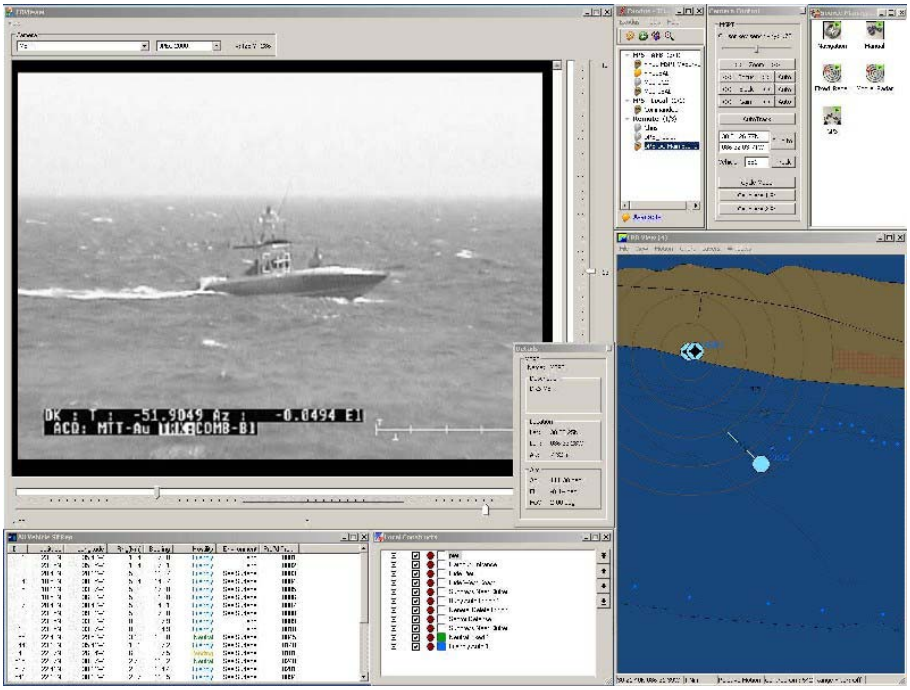

Figure 3. A screenshot from the InSITE Force Protection System shows the integration of real-time video with conventional target tracking. The ability to automatically cue the optical sensor to follow a nominated radar track is a major aid to classification.

The key functions provided by the command and control element are as follows.

1. Data collection. This includes the assimilation of data from the range of locally connected sensors, from connected surveillance systems and other manual inputs. Each of the individual sensor systems will provide a stream of data that can be reduced to a state estimate (and potentially other information) for a series of sensed objects. The use of standard Ethernet type interfaces taken from the latest military systems maximises the range of sensors that can be supported.

2. Sensor tasking. Some sensors have poor field of view and need to be directed to the parts of a scene for which more information is required. The best example of this would be use of high quality video to aid in the classification process – with the video requiring human interpretation. The direction of such sensors can be automated to follow high threat tracks that have been identified from other sensor sources.
3. Picture compilation. Data from all available sensors must be assimilated into a common picture. The benefits from presenting the data as a single common tactical picture include reduced workload compared with the need to monitor multiple sensor inputs and improved clarity. The tactical picture is presented as a labelled plan display with the option of using a range of established symbologies include MIL-STD 2525B, NTDS or user defined symbols.
4. Target identification. The operator needs to know the identification of all the objects shown in the tactical picture, based on all the information available. This needs to be as automated as possible and will provide a first step filtering process in that unidentified objects will generally pose a threat until positively identified. Some manual intervention may be needed here – e.g. to assess a video feed but this is greatly simplified where automatic collection of the video data is performed.
5. Threat assessment. The system applies threat assessments based on proximity to protected areas using predicted time to intercept or predicted time for weapon intercept. These are based on current course and speed of individual tracks. This process automatically generates a series of prioritised alerts – each of which has an associated textual description and recommended or required action. The use of nested areas and alert levels allows the operators to define a multi-layer defence approach.

The integrated, open systems architecture approach in the C2 will allow for the incorporation of new algorithms as they become available. These might include ;

- Improved sensor processing algorithms. This would cover the quality of extracted track data and the automation of the extraction process for image type sensors.
- Improved data fusion algorithms leading to improvements of the quality of the tactical picture.
- Improvements to the classification algorithms and improvements to threat assessments using factors such as track behaviour and other non-sensor inputs.

4.0 THE ROLE OF SIMULATION AND EXTENSIBLE ARCHITECTURES

In Section 2 the changing nature of the threat and its resultant impact on the ‘battlespace’ of interest was discussed. The large number of potential threat scenarios means that the range of response and of potential agencies involved, military and civilian, are considerable and understanding both the desired system capabilities and their effectiveness is difficult to grasp.

Within the conventional military domain it has been accepted that central to any Capability System Engineering Process, and the required exploration of threat and response space, is the role of simulation and modelling – the ubiquitous synthetic environment. That lesson is equally applicable for the domain of interest here – Defence Against Terrorism.

The diverse threat and range of effects that may result demands the adoption of flexible, extensible architectural concepts to provide robustness of solution both now and through time. This too is a lesson that has been learnt within the military environment where the significant levels of investment and required service lifetimes have required pro-active through life management consideration during the formulation of architectural solutions.

The following sub-sections will discuss each of these topics in turn.

4.1 Simulation

Synthetic environments allow a range of different users to share a consistent view of the issue being examined, permitting effective visualisation and assessment of both the issues and possible solutions. This stimulates understanding of the issues, especially the interactions of cause and effect within complex systems. Within the synthetic environment people and real (live) equipment interact with models and simulations developed to a degree of representation commensurate with the issues being examined. For more information on Synthetic Environment Based Acquisition (SEBA) and the role of synthetic environments see [3].

Within the context of 'Defence against Terrorism' the use of synthetic environment technology has a role to play in support of

- Assessment of the threat by exercise (role-play) to establish current defence effectiveness
- Assessment of the effectiveness of solution concepts (equipment, operational process and procedures, organisation and training - in the military domain this would be across all Lines of Development) in response to such threats, and setting automation goals as a result
- Assessment of people by the provision of a training and rehearsal environment

It is suggested, in [[1]], that the usual methods for reducing a problem to one that can be addressed by systems engineering methods involving such techniques as operational analysis, synthetic environments, and human factors may not be sufficient to address the challenges created by new and emerging threats.

There is an important need to characterise the threat and to understand the risks of failure to identify all aspects of a threat. It is proposed in [[1]] that use of the Threat Space construct and cluster analysis can provide significant new levels of insight into the nature of specific threats, and the reference goes on to describe three techniques that can be used to analyse the decomposed and clustered threat data. These are presented in Figure 4 below.

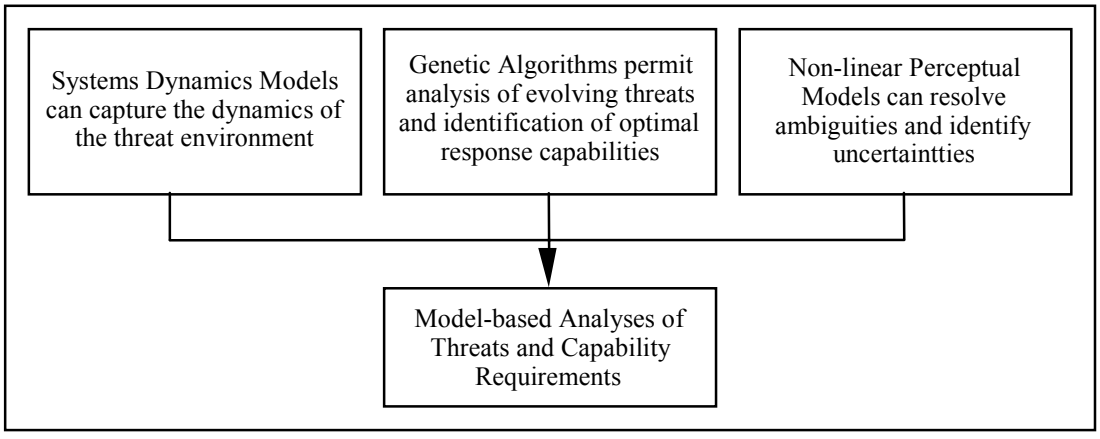

Figure 4: Candidate Threat Analysis Techniques based on [1]

The products of such analytic processes can then be used within a conventional multi-layered modelling schema to help identify required capabilities, exercise potential solutions and because of the inherent difficulty in fully characterising the threat provide a test environment in which the potential impact of any such incompleteness can be investigated.

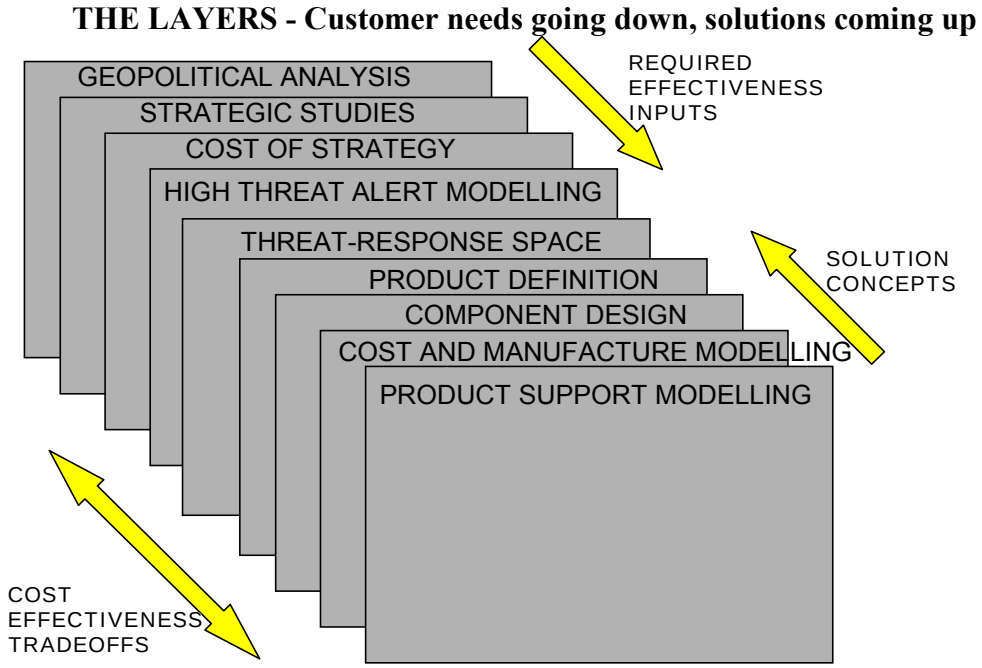

Figure 5: AMS Synthetic Environment multi-layer model for 'Defence against Terrorism'

Within AMS we have developed a Synthetic Environment based Battlespace Management Evaluation Centre (BMEC), a highly flexible and re-configurable facility for full-lifecycle support of emerging C4ISR system solutions and concepts. It is designed to support large-scale systems integration experiments involving, where necessary, links to federates available from NITEworks, MoD, DSTL and/or other companies. It is a key tool in delivering the right capability at the right price to meet the evolving requirements of the defence customer. Modern warfare is becoming more unpredictable and as the nature of threats change, we need to find solutions that may be as radical as the questions being asked.

Increasingly defence customers are looking for:

- The ability to "Fight Smarter" by better use of existing defence assets to achieve more with less
- More efficient and timely use of information throughout the Battlespace
- Better, more joined up capability (SE based acquisition for UK MoD)
- Integrated equipment of varying ages and capability
- Integrated sensors, decision makers and weapons
- Complete integration and acceptance capability over the full operational envelope

The BMEC provides an evaluation environment that is generic, re-configurable and allows cost-effective evaluation of Battlespace concepts across programme boundaries. It enables examination of problems from a system of systems view across the full Battlespace (as well as platform-centric). The BMEC facilitates the evaluation of operational effectiveness using objective experiments. This promotes early visualisation of problems and stimulates intense stakeholder involvement.

For example, within the 'Defence Against Terror' domain a larger scale of surveillance task is envisaged. This is likely to impose much greater demands on the human operators. The solution response would seek to provide increased automation for fusion of data and information from a wider range of sources and automated situation assessment to provide timely warning of threats. These are key areas of research

within AMS and in the wider research community and ones where the development of counter terrorism systems could benefit significantly.

A BMEC framework would provide a reference against which to assess where that balance between human and automation should be struck, it also provides a vehicle to train and develop users of the operational systems. The technology used and the architectural concepts employed within the BMEC are readily portable to the 'Defence Against Terrorism' domain.

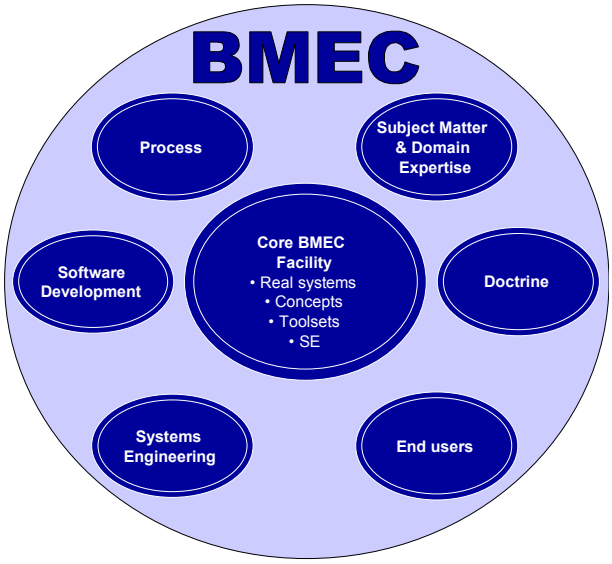

Figure 6 : The Battlefield Modelling and Evaluation Capability at AMS is an established engineering facility equally useful for Defence Against Terrorism applications as conventional military problems.

The architectural approach is based upon the use of Open and Standard Interfaces, and hosts leading edge data collection, analysis, rapid prototyping and scenario management tools and available visual models and databases. It is then populated with real / emulated C2/C4I systems (developing or existing) from the relevant domains. Domain knowledge and doctrine is provided by Subject Matter Experts.

Although originally directed at the classic military scenario the methodology and the tools are directly exploitable for the 'Defence Against Terror' domain. Where greater effort will be needed is in the modelling of the threat – in the terrorism environment actions are more likely to be initiated by individual or small groups and not fit so readily into classic command and control models. Role-playing of terrorists can be used to stimulate scenarios and to support training and rehearsal.

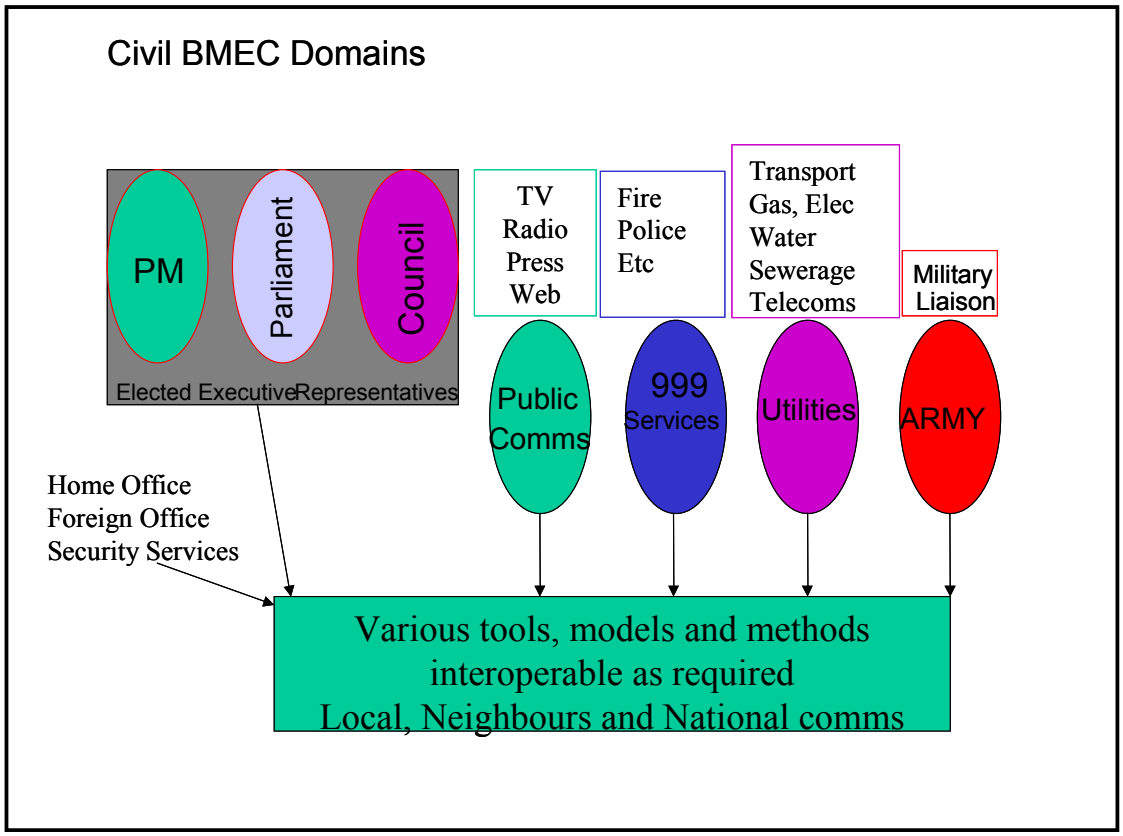

Figure 7. The integrated synthetic environment concepts developed in the BMEC could equally be applied to the diverse organisations involved in ensuring security.

Where the military BMEC recognises and populates military domains (land, sea, air, joint,..) a civil BMEC would broaden the domains covered to encompass relevant civil agencies.

4.2 Open, Extensible Architecture

Within SEBA, the concept architecture is represented in the synthetic environment, and will evolve to wards the design architecture and eventually the deployed system architecture

The diverse threat and range of effects that may result demands the adoption of flexible, extensible architectural concepts to provide robustness of solution both now and through time. This too is a lesson that has been learnt within the military environment where the significant levels of investment and required service lifetimes have required pro-active through life management consideration during the formulation of architectural solutions.

The architectural solutions will need to be -

- Scaleable – have the capability to support deployment of resources at a level commensurate with the perceived threat
- Robust – have the capability to perform effectively despite the degradation that may result from damage resulting from the threat
- Flexible – have the capability in the varied circumstances that may result from changing nature of the threat and its inherent variability

- Integrable – have the capability to deploy and integrate with existing legacy infrastructures thus minimising investment

In addition the solutions must support audit and transparency of the decision-making process and provide information management and shared awareness to all agencies and authorities.

These are all familiar requirements within the military domain where the response has been the increasing pursuit of technologies that support the generation of open, modular, decentralised and adaptive systems. This does not mean that there are not challenges, in particular the soft issues.

Inevitably there will be a need for increased automation to assist the users address the increasingly complex situations that we will need to address and key technologies that will support this are discussed further in Section 5.

Standards and processes are also important for an integrated solution, and the adoption of Open standards and the definition of IT system architectures and middleware that supports them is a common approach.

Perhaps most important is the adoption of enduring architectural principles against which the architecture and the selection of COTS / MOTS components to populate it will be judged. The following principles were seeded by those expounded by the Open System Group. The principles cover four areas:

- Operational Principles
- Data Principles
- Application Principles
- Technical Principles

Examples of Operational principles include:

- Information management. All users participate in the management of information needed to accomplish operational objectives. The exploitation of information will be key and to ensure it is aligned with an operation, all users must be involved with all aspects of the information environment
- Collaborative working. Users will participate in a collaborative working environment to minimise the time taken to make decisions, plan and re-plan operations. This will have implications on the necessary communications infrastructure
- Shared awareness. Users will need to have an awareness of each others perceptions of the situation. This implies access to coherent situational information using all available sources

Examples of Data principles are:

- Data is an asset. Data is an asset that has value to the organisation and is managed accordingly. The purpose of data is to aid decision-making and accurate timely data is critical to accurate timely decisions.
- Data is shared. Users have access to the data necessary to perform their duties and data is therefore shared.
- Data is accessible. Data is accessible for users to perform their functions. Wide access to data leads to efficiency and effectiveness in decision-making

Examples of Application principles are:

- Technology independence. Applications are independent of specific technology choices and therefore can operate on a variety of technology platforms. This allows applications to be

developed, upgraded, and operated in the most cost-effective way, otherwise technology which is subject to continual obsolescence and vendor dependence becomes the driver rather than the user requirements themselves. For example this principle requires the use of standards that support portability and the use of middleware to decouple applications from specific platforms and technologies.

- Ease of use. Applications are easy to use, with the underlying technology transparent to the user, so they can concentrate on tasks at hand.

Examples of Technical principles are:

- Control of technical diversity. Technological diversity is controlled to minimise non-trivial cost of maintaining expertise in and connectivity between multiple processing environments
- Interoperability. Software and hardware should conform to defined standards that promote interoperability for data, applications and technology
- Integration. Architecture should support an effective integration of various products, interfaces and infrastructures. Architecture that supports component integration will be flexible to accommodating further capabilities and adapting to change.

5.0 TECHNOLOGY EVOLUTION AND THE POTENTIAL FOR INCREASED AUTOMATION

The scope of the problem (Section 2) and the assessment of the requirements for technologies needed to support defence against terrorism in Section 3 provides a clear indication of the need to reduce the load on operators through greater automation, especially in the process of assimilating information and assessing threats. Put simply with a large number of inputs, the need to respond quickly and to provide continuous monitoring against potentially unknown threats for 24 hours a day the need for a greater degree of automation is inevitable. This is a theme common with much work in the defence community and the problems that need to be solved are broadly similar.

The key areas where automation is required are in the assimilation or fusion of multiple information sources into a coherent picture and in the assessment of threats based on all the information available. Much has been written about the subject of data and information fusion and several attempts have been made to develop a model that allows for categorisation of fusion into different levels. The best of these and that most widely accepted is that developed by the US DoD Joint laboratories in [[2]]. These models reflect the fact that data fusion is used to describe a wide range of different processes.

The fusion of data from multiple sensors (at both the measurement and track levels) is relatively mature and such capabilities exist in many military picture compilation systems. By contrast the ability to automate fusion processes in the information domain is still an embryonic capability with much useful work in the research community but little fielded capability. It is in this area of information fusion that significant technological advances could impact most on systems for defence against terrorism.

The reason for this is the heavy reliance that we will otherwise place on human contributions to classify and assess potential threats – and the risks that this poses. Areas where improvements can be expected include

- Better identification and classification of targets in a highly cluttered environment. Techniques that rely predominantly on kinematics and very limited physical data to classify targets will always be deficient – and often many more sources of data will be available that could assist in this process. More detailed physical characteristics data describing shape and other attributes combined with intelligence and other relatively unstructured inputs could all be used and clearly would in a human reasoning approach.

- Perhaps most importantly the ability to assess threats based on all available information. This will be critical when two small surface craft might appear equivalent on the basis of direct observation but other factors such as behaviour, known history, gaps in information and intelligence might distinguish one as more probably a terrorist threat and worthy of further investigation.

We can see from this that satisfactory solutions to the situational awareness problem will need capabilities that are not yet well developed.

- The fusion of sensor derived, non-sensory and a priori data to provide the best possible estimate of position, motion and identity of all objects within the domain of interest
- The ability to consider relationships between entities that are being tracked.
- The ability to address potentially very high levels of uncertainty
- The ability to monitor and predict likely actions and hence predict the threat based on more than proximity measures

In addressing the terrorist threat we also need to consider a wide range of timelines for analysis and response. In a military context the distinction would be made between strategic and tactical timescales with a command hierarchy in place to address this and to a degree different systems being used. For defence against terrorism (e.g. protection of a point of vulnerability such as a port or harbour) this distinction is likely to be less clear-cut. However the assessment of information gathered over a long timescale and potentially from a wide geographical base is likely to be extremely important if the threat is to be addressed on an intelligence-led basis as well as a direct tactical response.

Operating over longer timescales the emphasis will be on gathering and analysing information that may help to identify a concealed threat that may only emerge very slowly. The targets will not be well defined and we may not actually know what to look for. This type of problem falls into the a very large class of problems for which the generic solutions termed information fusion may be appropriate. These problems typically involve the sifting and analysis of very large quantities of unstructured or irregular data to produce some insight into a particular situation. These are not real-time problems and currently might involve analysis over a period of hours or days.

But the time element is important in that the inputs may be recently collected data or data collected at any time in the past and filed for future use. There is a key issue here that it may be impossible to relate an item of data to a particular use or situation at the time it is collected or filed and the important relationships may only be known at some potentially much later time.

The technologies that are considered relevant include :

- Probabilistic or Bayesian networks, that can draw inferences from apparently unconnected information sources
- Data mining and pattern matching technologies that can explore very large volumes of data seeking to identify patterns
- Intelligent agents that in some respects mimic the exploratory behaviour that we might ourselves adopt in seeking to address such problems.
- Novelty detection – identifying the unusual and unexpected.

AMS has recognised the important of data and information fusion technologies and is actively participating in research in these specialist areas. A major initiative in this areas is the Distributed Data and Information Systems strategic programme established with BAE SYSTEMS and Southampton University Department of Computer Science. This innovative partnership will fund fundamental new work in a variety of areas specifically targeted at satisfying some of the emerging requirements that have recently been characterised.

6.0 CONCLUSIONS

There is no doubt that the emergence of a new, truly global terrorist threat poses new challenges both in terms of the type of response needed and the technologies that will be needed to support them. The sheer scale of the problem in terms of nature and origin of individual attacks will place enormous emphasis on intelligence driven approaches but even so round the clock surveillance over wide areas is likely to be a common requirement in future. The response must equally be balanced – an over-reaction to a perceived threat would in itself cause damage to the society that it is aiming to protect.

There are key challenges to be addressed that relate to the way defence against terrorism systems will be used. The operational concepts have in many cases still to be defined but it is clear that they will involve multiple agencies most probably operating in a decentralized fashion rather than a strict hierarchical control structure. Existing surveillance systems and facilities will need to be incorporated (and potentially updated) rather than replaced.

Technology will play a key role in supporting acceptable responses to the growing threats. In [4] it is stated that "Technology itself cannot guarantee security, but without the support of technology it is impossible." The challenge posed in this paper is the extent to which military systems and technologies can be used as part of the system solutions required and the answer is clearly that yes they can – although there will be a growing need for greater degrees of automation.

System concepts for defence against terrorism are only just now starting to evolve and be defined. It is clear that there is much more work to be done in this area. In this paper we describe a system for the protection of high value assets in ports and harbours. The same concept could easily be modified to address the protection of other high profile targets. But this only represents a small element of the total problem. The development of system concepts will need to be scenario driven – and this will be effective only if we take a wide enough view of the potential forms of attack.

As with military systems the use of Synthetic Environments and simulation can help in the definition of system concepts, operational processes and procedures.

Military surveillance, situational assessment, command and control systems do provide a useful basis for at least one sub-set of the problems. These systems have the advantage of considerable maturity and the latest versions have been built using open systems concepts making them much easier to evolve and extend than would have been the case in the past. The AMS InSITE products provide an excellent example of this. However it is equally clear that existing systems that are not built on open architecture concepts will lack the flexibility and not provide such good starting points.

The technology gaps that we need to fill largely relate to greater degrees of automation, allowing effective wide area surveillance to be achieved round the clock without unreasonable manpower requirements – and without high levels of false alarm. Potential solutions lie in better data and information fusion technologies and inference based decision support tools. It is perhaps interesting that similar requirements have emerged in the military field, based on the need to keep personnel out of harms way and on the need to achieve more with fewer people.

Our approach in AMS is to build on the capabilities that we already have and produce an integrated solution concept to one particular set of surveillance requirements. We have an architecture that allows for expansion and evolution both to extend the scope of the surveillance and to introduce new information technologies as they become available. This approach has been shown to be successful and this success stems from the following.

- Our background in military surveillance, command and control systems provided a mature starting point for the solution

- The capability we had was easily adaptable to address the different requirements
- We realised early on the need for an integrated and extensible approach – with the potential for interoperability with existing facilities such as vessel traffic management systems
- Our investment in developing the capabilities and technologies needed in future defence systems also provides an insight into the potential for system solutions to operate with reduced need for large numbers of highly skilled operators.
- As a major user of synthetic environment capabilities we understand the benefit such tools can provide in exploring future system concepts and establishing operational procedures – without the need to deploy the systems and without the ability to rehearse against real threats.

REFERENCES

[1] A.E.R Woodcock, "How to manage the uncertainty of emergent threats in capability based acquisition" Unpublished Technical Report, 2004

[2] Steinberg, A.N., Bowman, C.L., and White, F.E., "Revisions to the JDL Data Fusion Model", in Sensor Fusion: Architectures, Algorithms, and Applications, Proceedings of the SPIE, Vol. 3719, 1999.

[3] UK Ministry of Defence Synthetic Environment Based Acquisition website. www.mod.uk/issues/simulation/seba.htm

[4] Research for a Secure Europe. Report of the Group of Personalities in the field of Security Research. European Communities, 2004.

[5] Outline NATO Staff Target – Components for Unmanned Underwater Vehicles for Vessel Protection in Ports and Harbours. AC/141 (NG/3) D/20